Digitale Bibliothek Braunschweig

Herrn Director Dr. A. Wernicke
freundlichst vom Verf.
Sammlung
V. L. 1179.

Ueber eine Erweiterung des Symbols $(\mathfrak{a}, \mathfrak{b})$ in der Theorie der Moduln.

Von

R. Dedekind.

BIBLIOTHEK.
TECHN. HOCHSCHULE
BRAUNSCHWEIG.

Aus den Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen.
Mathematisch-physikalische Klasse. 1895. Heft 2.

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

Aus den Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen.
Mathematisch-physikalische Klasse. 1895. Heft 2.

Geschenk

BIBLIOTHEK.
HERZOGL.
TECHN. HOCHSCHULE
CAROLO-WILHELMINA
BRAUNSCHWEIG.

Ueber eine Erweiterung des Symbols (a, b) in der Theorie der Moduln.

Von

R. Dedekind in Braunschweig, ausw. Mitglied.

(Vorgelegt am 11. Mai 1895 vom vorsitzenden Secretär.)

Am Schlusse des Vorwortes zu meiner Abhandlung Ueber die Discriminanten endlicher Körper, welche der Königl. Gesellschaft am 5. August 1882 vorgelegt und in den Bd. 29 der Abhandlungen aufgenommen ist, habe ich hervorgehoben, daß alle in ihr gewonnenen Resultate einer wichtigen Verallgemeinerung fähig sind, zu welcher man dadurch gelangt, daß man den endlichen Körper Ω nicht nur auf den Körper der rationalen Zahlen, sondern auch auf jeden in Ω als Divisor enthaltenen Körper bezieht, wobei neben den gewöhnlichen Normen, Discriminanten, Spuren auch partielle oder relative, auf diesen Körper bezügliche Normen u. s. w. einzuführen, und gewisse rationale Zahlen durch Ideale dieses Körpers zu ersetzen sind. Die Durchführung dieser Verallgemeinerung erfordert, wie ich damals bemerkt habe, einige vorbereitende Untersuchungen, welche aber auch ein selbständiges Interesse darbieten, und unter diesen befindet sich die in der Ueberschrift genannte Erweiterung des in der Modultheorie auftretenden Symbols $(\mathfrak{a}, \mathfrak{b})$, welche den Hauptgegenstand der folgenden Mittheilung bildet. Hierbei muß ich die Kenntniß des letzten Supplementes der vierten Auflage (1894) von Dirichlet's Vorlesungen über Zahlentheorie voraussetzen, welche ich kurz mit D. citiren werde.

§ 1.

Der Grundgedanke unserer Untersuchung ist der folgende. Aus dem Begriffe eines Moduls (D. § 168) ergiebt sich eine unmittelbare Beziehung desselben zu dem Körper R der rationalen Zahlen, welche darin besteht, daß jede Zahl α eines Moduls $\mathfrak{a}$ durch Multiplication mit jeder ganzen rationalen Zahl a immer in

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

eine Zahl $\alpha\alpha$ desselben Moduls $\mathfrak{a}$ verwandelt wird; bezeichnet man mit $\mathfrak{z}$ den Inbegriff [1] aller ganzen Zahlen des Körpers R, so kann man diese Eigenschaft auch so aussprechen (D. S. 500), daß das Product $\mathfrak{z}\mathfrak{a}$ stets theilbar durch $\mathfrak{a}$ ist. Auf dieser Eigenschaft beruht ein großer Theil der allgemeinen Modultheorie. Ersetzen wir nun den Körper R durch einen beliebig gewählten endlichen Körper Z, der aber ungeändert beibehalten wird, und bezeichnen wir mit $\mathfrak{z}$ den Inbegriff aller in ihm enthaltenen ganzen Zahlen, so soll im Folgenden die Theorie aller derjenigen Moduln $\mathfrak{a}$ entwickelt werden, welche die Eigenschaft besitzen, daß $\mathfrak{z}\mathfrak{a}$ durch $\mathfrak{a}$ theilbar ist. In unseren Zeichen wird dies durch

$$\mathfrak{z}\mathfrak{a} > \mathfrak{a} \quad \text{oder} \quad \mathfrak{z} > \mathfrak{a}^0 \tag{1}$$

ausgedrückt, wo $\mathfrak{a}^0$ die Ordnung des Moduls $\mathfrak{a}$ bedeutet (D. S. 505). Da in $\mathfrak{z}$ auch die Zahl 1 enthalten, also immer $\mathfrak{a} > \mathfrak{z}\mathfrak{a}$ ist, so ist diese Eigenschaft auch gleichbedeutend mit

$$\mathfrak{z}\mathfrak{a} = \mathfrak{a}. \tag{2}$$

Man kann sie auch so aussprechen, daß jede auf den Modul $\mathfrak{a}$ bezügliche Congruenz mit jeder ganzen Zahl des Körpers Z multiplicirt werden darf (D. S. 508). Wenn nun der Modul $\mathfrak{b}$ dieselbe Eigenschaft besitzt, so ergiebt sich aus den allgemeinen Sätzen (D. S. 502, 500, 504)

$$\mathfrak{z}(\mathfrak{a}+\mathfrak{b}) = \mathfrak{z}\mathfrak{a}+\mathfrak{z}\mathfrak{b}, \quad \mathfrak{z}(\mathfrak{a}-\mathfrak{b}) > \mathfrak{z}\mathfrak{a}-\mathfrak{z}\mathfrak{b}, \tag{3}$$

$$\mathfrak{z}(\mathfrak{a}\mathfrak{b}) = (\mathfrak{z}\mathfrak{a})\mathfrak{b}, \quad \mathfrak{z}\left(\frac{\mathfrak{b}}{\mathfrak{a}}\right) > \frac{\mathfrak{z}\mathfrak{b}}{\mathfrak{a}}, \tag{4}$$

daß auch die vier Moduln $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}-\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$ und $\mathfrak{b}:\mathfrak{a}$ von derselben Beschaffenheit sind. Mit Rücksicht auf diese Reproduction durch alle Modul-Operationen wollen wir der Kürze wegen ein für allemal festsetzen, daß unter einem Modul schlechthin, falls nicht das Gegentheil ausdrücklich bemerkt wird, im Folgenden stets ein solcher Modul $\mathfrak{a}$ verstanden werden soll, welcher die durch (1) oder (2) ausgedrückte Eigenschaft besitzt. —

Wir betrachten zunächst alle diejenigen endlichen, von Null verschiedenen Moduln, deren Zahlen dem Körper Z angehören. Zu der Bezeichnung dieser Moduln soll in der Regel die zweite Hälfte des lateinischen Alphabetes dienen, während die Buchstaben der ersten Hälfte meistens Zahlen des Körpers Z bedeuten. Da die Ordnung x^0 eines solchen Moduls x aus lauter ganzen Zahlen besteht (D. S. 527), welche offenbar in Z, also auch in $\mathfrak{z}$ enthalten sind, so ist $x^0 > \mathfrak{z}$, und da zufolge

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

(1) auch $z > x^0$ ist, so folgt $x^0 = z$, mithin ist jeder solche Modul x ein Idealbruch (D. S. 560. Anm.). Dieser Fall ist so wichtig für unsere Untersuchung, daß ich noch einige Worte zur Erläuterung hinzufügen will. Wenn x ein ganzer Modul, also $x > z$ ist, so ist er offenbar ein Ideal (D. S. 551); hierbei bemerke ich ein für allemal, daß immer nur von solchen Idealen und Idealbrüchen die Rede sein wird, welche im Körper Z enthalten sind, was also künftig stets hinzuzudenken ist. Wenn aber der endliche Modul x auch gebrochene Zahlen enthält, so kann man eine von Null verschiedene ganze Zahl a des Körpers Z so wählen, daß alle Basiszahlen von x durch Multiplication mit a in ganze Zahlen verwandelt werden, und folglich xa ein Ideal y wird; allgemeiner, es giebt unendlich viele Paare von Idealen u, v (z. B. $u = za$, $v = y$), welche der Bedingung $xu = v$ genügen, woraus $x = v : u = vu^{-1}$, also auch $x^{-1} = z : x = uv^{-1} = u : v$, und $xx^{-1} = z$ folgt (D. S. 553, 506, 507). Unter allen diesen Paaren u, v giebt es ein einziges, welches aus zwei relativen Primidealen u_0, v_0 besteht (D. S. 556), und jedes Paar ist von der Form $u = wu_0$, $v = wv_0$, wo $w = u + v$ ein willkürliches Ideal bedeutet; zugleich leuchtet ein, daß $u_0 = z - x^{-1}$ der Inbegriff aller oben mit a bezeichneten Zahlen (einschließlich $a = 0$), und ebenso $v_0 = z - x$, ferner $u_0^{-1} = z + x$, $v_0^{-1} = z + x^{-1}$ ist. —

Aus den soeben betrachteten Moduln x bilden wir jetzt alle Moduln $\mathfrak{p}$ von der allgemeineren Form

$$\mathfrak{p} = x\alpha, \tag{5}$$

wo α jede beliebige, von Null verschiedene Zahl innerhalb oder außerhalb Z bedeutet. Diese Moduln $\mathfrak{p}$ wollen wir kurz einfache Moduln nennen, weil sie für unsere Untersuchung genau dieselbe Bedeutung besitzen, wie die von Null verschiedenen eingliedrigen Moduln für die allgemeine Modultheorie (D. S. 494), und weil sie mit diesen letzteren zusammenfallen, wenn Z der Körper R der rationalen Zahlen ist.[1]) Jeder einfache Modul $\mathfrak{p}$ ist offenbar ein endlicher, von Null verschiedener Modul, in welchem jedes Zahlenpaar ein nach Z reducibeles System bildet (D. S. 466), und man überzeugt sich leicht, daß hierdurch umgekehrt der gemeinsame Charakter aller einfachen Moduln auf invariante Weise bestimmt ist. Offenbar läßt sich aber jeder einfache Modul $\mathfrak{p}$ auf unendlich viele verschiedene Arten in der Form (5) darstellen; ist nämlich y irgend ein mit x äquivalenter Idealbruch (D. S. 579),

1) Die Wahl des Buchstaben $\mathfrak{p}$ soll also keineswegs an Primideale erinnern.

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

also $x = yc$, wo c irgend eine von Null verschiedene Zahl in Z bedeutet, so wird $\mathfrak{p} = y\beta$, wo $\beta = c\alpha$; man darf daher bei der Darstellung (5) auch immer annehmen, dass x ein ganzer Idealbruch, d. h. ein Ideal ist.

Zugleich leuchtet ein, daß jeder einfache Modul $\mathfrak{p}$ ein eigentlicher Modul (D. S. 506), dass nämlich

$$\mathfrak{p}^0 = z = \mathfrak{p}\mathfrak{p}^{-1}, \quad \mathfrak{p}^{-1} = x^{-1}\alpha^{-1} \tag{6}$$

ist, und ebenso, daß Producte und Quotienten von einfachen Moduln wieder einfache Moduln sind. Hieraus folgt auch leicht, daß immer

$$(\mathfrak{a}-\mathfrak{b})\mathfrak{p} = \mathfrak{a}\mathfrak{p}-\mathfrak{b}\mathfrak{p} \tag{7}$$

ist; denn nach der allgemeinen Modultheorie (D. S. 502) ist die linke Seite theilbar durch die rechte, und ebenso ist $(\mathfrak{a}\mathfrak{p}-\mathfrak{b}\mathfrak{p})\mathfrak{p}^{-1}$ theilbar durch den Modul $\mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1}-\mathfrak{b}\mathfrak{p}\mathfrak{p}^{-1}$, d. h. durch $\mathfrak{a}-\mathfrak{b}$, woraus durch Multiplication mit $\mathfrak{p}$ folgt, daß auch die rechte Seite unserer Gleichung (7) durch die linke theilbar ist, w. z. b. w. Auf dieselbe Weise ergiebt sich, daß aus $\mathfrak{a}\mathfrak{p} > \mathfrak{b}\mathfrak{p}$ stets $\mathfrak{a} > \mathfrak{b}$, und aus $\mathfrak{a}\mathfrak{p} = \mathfrak{b}\mathfrak{p}$ stets $\mathfrak{a} = \mathfrak{b}$ folgt.

§ 2.

Wir wenden uns jetzt zum Beweise von Sätzen, auf denen die Einführung eines neuen Symbols beruht, und bei welchen die Analogie zwischen unseren einfachen Moduln und den eingliedrigen Moduln der allgemeinen Theorie noch deutlicher hervortritt (vergl. D. S. 514).

I. Jedes von Null verschiedene Vielfache $\mathfrak{q}$ eines einfachen Moduls $\mathfrak{p}$ ist ein einfacher Modul von der Form

$$\mathfrak{q} = u\mathfrak{p}, \tag{8}$$

wo u ein Ideal bedeutet, dessen Norm

$$(z, u) = N(u) = (\mathfrak{p}, \mathfrak{q}) \tag{9}$$

ist.

Denn aus der Theilbarkeit von $\mathfrak{q}$ durch $\mathfrak{p}$ folgt durch Multiplication mit $\mathfrak{p}^{-1}$, daß der von Null verschiedene Modul $\mathfrak{q}\mathfrak{p}^{-1}$ durch z theilbar, also ein Ideal u ist, woraus sich (8) ergiebt; da ferner $\mathfrak{p}$ von der Form (5) ist, wo x als ein Ideal angenommen werden darf, so ergiebt sich nach bekannten Sätzen (D. S. 510, 564)

$$(\mathfrak{p}, \mathfrak{q}) = (x\alpha, ux\alpha) = (x, ux) = N(u),$$

w. z. b. w.

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

Wir bemerken zunächst, daß das in (8) auftretende Ideal u durch $\mathfrak{p}$ und $\mathfrak{q}$ vollständig bestimmt ist, weil aus (8) durch Multiplication mit $\mathfrak{p}^{-1}$ wieder $u = \mathfrak{q}\mathfrak{p}^{-1}$ folgt. Bedeutet ferner π irgend eine von Null verschiedene Zahl in $\mathfrak{p}$, so ist $\varepsilon\pi > \mathfrak{p}$, also $\varepsilon\pi = u\mathfrak{p}$, wo $u = \pi\mathfrak{p}^{-1}$ ein Ideal; offenbar entsprechen allen Zahlen π lauter äquivalente Ideale u (D. S. 573), und umgekehrt, wenn das Ideal u' mit u äquivalent, also $u' = cu$ ist, wo c eine Zahl des Körpers Z bedeutet, so ist die Zahl $\pi' = c\pi$ in $\mathfrak{p}$ enthalten, und $u' = \pi'\mathfrak{p}^{-1}$; man kann daher (D. S. 579) die Zahl π aus $\mathfrak{p}$ auch immer so auswählen, daß $\pi\mathfrak{p}^{-1}$ relatives Primideal zu irgend einem gegebenen Ideale wird.

Sodann benutzen wir den vorstehenden Satz, um für einen beliebigen Modul $\mathfrak{m}$ und einen einfachen Modul $\mathfrak{p}$ ein neues Symbol $(\mathfrak{p}; \mathfrak{m})$ zu erklären, in welchem wir die beiden Moduln nicht durch ein Komma, sondern durch ein Semikolon von einander trennen. Hierbei sind zwei Fälle zu unterscheiden, je nachdem $(\mathfrak{p}, \mathfrak{m}) > 0$ oder $= 0$ ist (D. S. 509). Da immer $(\mathfrak{p}, \mathfrak{m})\mathfrak{p}$ durch $\mathfrak{p}-\mathfrak{m}$ theilbar ist (D. S. 511), so ist im ersten Falle auch $\mathfrak{p}-\mathfrak{m}$ ein von Null verschiedenes Vielfache $\mathfrak{q}$ von $\mathfrak{p}$, und wir definiren $(\mathfrak{p}; \mathfrak{m})$ gemäß (8) als das durch die Gleichung

$$\mathfrak{p}-\mathfrak{m} = (\mathfrak{p}; \mathfrak{m})\mathfrak{p} \tag{10}$$

vollständig bestimmte Ideal[1])

$$(\mathfrak{p}; \mathfrak{m}) = (\mathfrak{p}-\mathfrak{m})\mathfrak{p}^{-1}, \tag{11}$$

und da immer $(\mathfrak{p}, \mathfrak{m}) = (\mathfrak{p}, \mathfrak{p}-\mathfrak{m})$ ist (D. S. 510), so folgt aus (9) auch

$$(\mathfrak{p}, \mathfrak{m}) = N(\mathfrak{p}; \mathfrak{m}). \tag{12}$$

Da umgekehrt, wenn $\mathfrak{p}-\mathfrak{m}$ von Null verschieden ist, zufolge (8) und (9) dasselbe auch von $(\mathfrak{p}, \mathfrak{m})$ gilt, so tritt der zweite Fall $(\mathfrak{p}, \mathfrak{m}) = 0$ stets und nur dann ein, wenn $\mathfrak{p}-\mathfrak{m} = 0$ ist, und dann wollen wir auch

$$(\mathfrak{p}; \mathfrak{m}) = 0 \tag{13}$$

setzen, weil hierdurch die Gleichungen (10), (11), (12) erhalten bleiben. In allen Fällen ist offenbar

$$(\mathfrak{p}; \mathfrak{m}) = (\mathfrak{p}; \mathfrak{p}-\mathfrak{m}). \tag{14}$$

Ebenso geht aus (10) hervor, daß die Gleichung

$$(\mathfrak{p}; \mathfrak{m}) = \varepsilon \text{ gleichbedeutend mit } \mathfrak{p} > \mathfrak{m} \tag{15}$$

1) Ist x ein Idealbruch, so ist z. B. $(\varepsilon; x) = v_0$, $(x; \varepsilon) = u_0$, wo u_0 und v_0 dieselbe Bedeutung für x haben, wie in § 1.

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

ist. Multiplicirt man ferner (10) mit einem beliebigen einfachen Modul $\mathfrak{p}'$, so folgt mit Rücksicht auf (7) der in allen Fällen geltende Satz

$$(\mathfrak{p}\mathfrak{p}';\ \mathfrak{m}\mathfrak{p}') = (\mathfrak{p};\ \mathfrak{m}). \tag{16}$$

Durch wiederholte Anwendung des Satzes I und der daraus gezogenen Folgerungen ergiebt sich der Satz

II. Sind $\mathfrak{a}, \mathfrak{b}$ beliebige Moduln, so ist $(\mathfrak{a}, \mathfrak{b})$ entweder $= 0$ oder die Norm eines Ideals u.

Ist nämlich $(\mathfrak{a}, \mathfrak{b}) = 1$, also $\mathfrak{a} > \mathfrak{b}$, so wird dem Satze durch $u = z$ genügt. Ist aber $(\mathfrak{a}, \mathfrak{b}) > 1$, so kann man aus $\mathfrak{a}$ immer ein System $\mathfrak{P}$ von einfachen Moduln $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_n$ in endlicher Anzahl n so auswählen, daß

$$\mathfrak{a} = (\mathfrak{a}-\mathfrak{b}) + \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_n \tag{17}$$

wird; denn wenn z. B. die Zahlen $\alpha_1, \alpha_2, \ldots \alpha_s$, wo $s = (\mathfrak{a}, \mathfrak{b})$, ein Restsystem von $\mathfrak{a}$ nach $\mathfrak{b}$ bilden (D. S. 509), so ist offenbar auch $\mathfrak{a} = (\mathfrak{a}-\mathfrak{b}) + z\alpha_1 + z\alpha_2 + \cdots + z\alpha_s$, und dies ist nur ein specieller Fall der allgemeinen Darstellung (17). Setzt man nun, wenn ν irgend eine der Zahlen $1, 2, \ldots n$ bedeutet,

$$\mathfrak{a}_{\nu-1} = (\mathfrak{a}-\mathfrak{b}) + \mathfrak{p}_\nu + \mathfrak{p}_{\nu+1} + \cdots + \mathfrak{p}_n \tag{18}$$

und außerdem $\mathfrak{a}_n = \mathfrak{a}-\mathfrak{b}$, so ist $\mathfrak{a}_0 = \mathfrak{a}$ und

$$\mathfrak{a}_{\nu-1} = \mathfrak{p}_\nu + \mathfrak{a}_\nu < \mathfrak{a}_\nu, \tag{19}$$

also nach bekannten Sätzen (D. S. 510)

$$(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{a}_0, \mathfrak{a}_n) = (\mathfrak{a}_0, \mathfrak{a}_1)(\mathfrak{a}_1, \mathfrak{a}_2)\ldots(\mathfrak{a}_{n-1}, \mathfrak{a}_n)$$

und mit Rücksicht auf (12)

$$(\mathfrak{a}_{\nu-1}, \mathfrak{a}_\nu) = (\mathfrak{p}_\nu + \mathfrak{a}_\nu, \mathfrak{a}_\nu) = (\mathfrak{p}_\nu, \mathfrak{a}_\nu) = N(\mathfrak{p}_\nu;\ \mathfrak{a}_\nu).$$

Setzt man daher das Idealproduct

$$(\mathfrak{p}_1;\ \mathfrak{a}_1)(\mathfrak{p}_2;\ \mathfrak{a}_2)\ldots(\mathfrak{p}_n;\ \mathfrak{a}_n) = u, \tag{20}$$

so folgt aus dem bekannten Satze über die Norm eines Productes (D. S. 564) das Resultat

$$(\mathfrak{a}, \mathfrak{b}) = N(u), \tag{21}$$

w. z. b. w.

Es liegt nun die Vermuthung sehr nahe, daß das in (20) gebildete Idealproduct u, dessen Norm $= (\mathfrak{a}, \mathfrak{b})$, sowohl von der Reihenfolge der in der Darstellung (17) des Moduls $\mathfrak{a}$ auftretenden einfachen Moduln $\mathfrak{p}_\nu$ als auch von der Auswahl des Systems $\mathfrak{P}$ dieser Moduln gänzlich unabhängig, also invariant

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

durch a und b bestimmt ist. Um dies zu beweisen, schicken wir folgenden Hülfssatz voraus:

III. Sind $\mathfrak{p}$, $\mathfrak{q}$ einfache Moduln, und setzt man zur Abkürzung

$$\mathfrak{p}' = \mathfrak{p} - (\mathfrak{q} + \mathfrak{m}),\ \mathfrak{q}' = \mathfrak{q} - (\mathfrak{p} + \mathfrak{m}), \tag{22}$$

wo $\mathfrak{m}$ ein beliebiger Modul, so ist

$$\mathfrak{q}'(\mathfrak{p} - \mathfrak{m}) = \mathfrak{p}'(\mathfrak{q} - \mathfrak{m}). \tag{23}$$

Dies ergiebt sich ziemlich leicht aus dem in der allgemeinen Modultheorie (D. S. 499) bewiesenen, für je drei Moduln $\mathfrak{m}$, $\mathfrak{p}$, $\mathfrak{q}$ gültigen Satze

$$(\mathfrak{p} + \mathfrak{m}) - (\mathfrak{q} + \mathfrak{m}) = \mathfrak{p}' + \mathfrak{m} = \mathfrak{q}' + \mathfrak{m}, \tag{24}$$

woraus wir die für unseren Zweck hinreichenden Folgerungen

$$\mathfrak{p}' > \mathfrak{q}' + \mathfrak{m},\ \mathfrak{q}' > \mathfrak{p}' + \mathfrak{m} \tag{25}$$

ziehen. Nehmen wir nun zunächst an, die Moduln $\mathfrak{p} - \mathfrak{m}$ und $\mathfrak{q} - \mathfrak{m}$ seien beide von Null verschieden, so gilt dasselbe auch von $\mathfrak{p}'$ und $\mathfrak{q}'$, weil zufolge (22) offenbar $\mathfrak{p} - \mathfrak{m} > \mathfrak{p}'$ und $\mathfrak{q} - \mathfrak{m} > \mathfrak{q}'$ ist; da ferner $\mathfrak{p}' > \mathfrak{p}$ und $\mathfrak{q}' > \mathfrak{q}$, so sind (nach dem Satze I) auch $\mathfrak{p}'$, $\mathfrak{q}'$, $\mathfrak{p} - \mathfrak{m}$, $\mathfrak{q} - \mathfrak{m}$ einfache Moduln, und man kann daher

$$\mathfrak{p} - \mathfrak{m} = p\mathfrak{p}',\ \mathfrak{q} - \mathfrak{m} = q\mathfrak{q}' \tag{26}$$

setzen, wo p, q Ideale bedeuten, deren Identität wir jetzt beweisen wollen. Aus der ersten der durch (25) ausgedrückten Theilbarkeiten ergiebt sich durch Multiplication mit q zunächst $q\mathfrak{p}' > q\mathfrak{q}' + q\mathfrak{m}$; beide Moduln $q\mathfrak{q}'$, $q\mathfrak{m}$ sind aber durch $\mathfrak{m}$ theilbar, der erstere zufolge (26), und der letztere, weil $q > z$ ist; mithin ist auch $q\mathfrak{p}' > \mathfrak{m}$, und da ferner $q\mathfrak{p}' > \mathfrak{p}' > \mathfrak{p}$, so ist $q\mathfrak{p}'$ ein gemeinsames Vielfaches von $\mathfrak{m}$ und $\mathfrak{p}$, also auch theilbar durch $\mathfrak{p} - \mathfrak{m}$, d. h. $q\mathfrak{p}' > p\mathfrak{p}'$, und hieraus ergiebt sich $q > p$, weil $\mathfrak{p}'$ ein einfacher Modul ist. Zufolge der Symmetrie ist ebenso $p > q$, also wirklich

$$p = q, \tag{27}$$

und der Satz (23) ist daher eine unmittelbare Folge von (26), w. z. b. w. Dieser Satz gilt aber auch dann, wenn man die obige Annahme fallen läßt, daß $\mathfrak{p} - \mathfrak{m}$ und $\mathfrak{q} - \mathfrak{m}$ beide von Null verschieden sind. Dies leuchtet unmittelbar ein, wenn beide Moduln $= 0$ sind. Wenn ferner $\mathfrak{p} - \mathfrak{m} = 0$, aber $\mathfrak{q} - \mathfrak{m}$, also auch $\mathfrak{q}'$ von Null verschieden ist, so behält das Ideal q seine Bedeutung, und der obige Beweis für die Theilbarkeit von $q\mathfrak{p}'$ durch $\mathfrak{p} - \mathfrak{m}$ bleibt

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

bestehen, mithin ist $\mathfrak{p}' = 0$, und der Satz (23) auch jetzt richtig, w. z. b. w.

Drückt man die in (23) auftretenden Moduln gemäß (10) aus, so nimmt unser Satz folgende Form an:

IV. Sind $\mathfrak{p}$, $\mathfrak{q}$ einfache Moduln, während $\mathfrak{m}$ einen beliebigen Modul bedeutet, so ist

$$(28) \qquad (\mathfrak{q};\ \mathfrak{p}+\mathfrak{m})\ (\mathfrak{p};\ \mathfrak{m}) = (\mathfrak{p};\ \mathfrak{q}+\mathfrak{m})\ (\mathfrak{q};\ \mathfrak{m}).$$

Mit Hülfe desselben beweisen wir leicht, daß die Reihenfolge, nach welcher aus den in (17) auftretenden einfachen Moduln $\mathfrak{p}_\nu$ die Moduln $\mathfrak{a}_\nu$ in (18), (19) und die Ideale $(\mathfrak{p}_\nu;\ \mathfrak{a}_\nu)$ gebildet werden, keinen Einfluß auf deren Product u in (20) ausübt. In der That, ändert man diese Reihenfolge nur soweit ab, daß zwei Nachbaren $\mathfrak{p}_{\mu-1}$ und $\mathfrak{p}_\mu$ ihre Plätze mit einander vertauschen, alle übrigen $\mathfrak{p}_\nu$ ihren Platz behaupten, so bleiben auch alle Moduln $\mathfrak{a}_\nu$ mit einziger Ausnahme von $\mathfrak{a}_{\mu-1}$ ungeändert, welcher in

$$(\mathfrak{a}-\mathfrak{b})+\mathfrak{p}_{\mu-1}+\mathfrak{p}_{\mu+1}+\cdots+\mathfrak{p}_n = \mathfrak{p}_{\mu-1}+\mathfrak{a}_\mu$$

übergeht; zugleich bleiben alle Factoren des Productes u in (20) ungeändert mit Ausnahme von

$$(\mathfrak{p}_{\mu-1};\ \mathfrak{a}_{\mu-1}) \text{ und } (\mathfrak{p}_\mu;\ \mathfrak{a}_\mu),$$

welche resp. in

$$(\mathfrak{p}_\mu;\ \mathfrak{p}_{\mu-1}+\mathfrak{a}_\mu) \text{ und } (\mathfrak{p}_{\mu-1};\ \mathfrak{a}_\mu)$$

übergehen; da aber $\mathfrak{a}_{\mu-1} = \mathfrak{p}_\mu + \mathfrak{a}_\mu$ ist, so folgt aus (28), wenn man $\mathfrak{q} = \mathfrak{p}_{\mu-1}$, $\mathfrak{p} = \mathfrak{p}_\mu$, $\mathfrak{m} = \mathfrak{a}_\mu$ setzt, daß das Product der beiden ersteren Moduln mit dem der beiden letzteren identisch ist, also das Product u ungeändert bleibt. Dasselbe gilt daher auch für jede Abänderung der Reihenfolge, weil eine solche bekanntlich immer durch fortgesetzte Vertauschung von zwei Nachbaren hervorgebracht werden kann, und wir dürfen daher sagen, das Idealproduct u entspreche dem Systeme $\mathfrak{P}$ der n einfachen Moduln $\mathfrak{p}_\nu$, welche in der Darstellung (17) des Moduls $\mathfrak{a}$ auftreten.

Noch leichter läßt sich nun zeigen, daß das Ideal u auch von der Auswahl des Systems $\mathfrak{P}$ unabhängig ist. Nehmen wir nämlich einmal an, es reiche schon das System $\mathfrak{P}_1$ der $n-1$ einfachen Moduln $\mathfrak{p}_2, \mathfrak{p}_3 \ldots \mathfrak{p}_n$ zu einer solchen Darstellung von $\mathfrak{a}$ aus, es sei also

$$(29) \qquad \mathfrak{a} = (\mathfrak{a}-\mathfrak{b})+\mathfrak{p}_2+\mathfrak{p}_3+\cdots+\mathfrak{p}_n,$$

so wird, wenn man zu $\mathfrak{P}_1$ einen beliebigen, durch $\mathfrak{a}$ theilbaren einfachen Modul $\mathfrak{p}_1$ hinzufügt, ein System $\mathfrak{P}$ von n einfachen

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

Moduln $\mathfrak{p}_\nu$ entstehen, welches der Bedingung (17) genügt, weil $\mathfrak{a} + \mathfrak{p}_1 = \mathfrak{a}$ ist. Behält man nun die früheren Bezeichnungen bei, so entspricht dem System $\mathfrak{P}_1$ das Idealproduct

$$u_1 = (\mathfrak{p}_2; \mathfrak{a}_2)\,(\mathfrak{p}_3; \mathfrak{a}_3) \ldots (\mathfrak{p}_n; \mathfrak{a}_n),$$

und folglich ist $u = (\mathfrak{p}_1; \mathfrak{a}_1)\, u_1$; da aber zufolge (29) schon $\mathfrak{a}_1 = \mathfrak{a}$, also auch $\mathfrak{p}_1 > \mathfrak{a}_1$ ist, so folgt aus (15), daß $(\mathfrak{p}_1; \mathfrak{a}_1) = z$, mithin $u_1 = u$ ist. Dasselbe ergiebt sich auch daraus, daß zufolge (21) gewiß $N(u) = N(u_1)$, also $N(\mathfrak{p}_1; \mathfrak{a}_1) = 1$ ist. Nennen wir der Kürze halber, indem wir die beiden Moduln $\mathfrak{a}$, $\mathfrak{b}$ festhalten, jedes System $\mathfrak{P}$ von n einfachen Moduln $\mathfrak{p}_\nu$, welches der Bedingung (17) genügt, ein vollständiges System, so können wir das eben gewonnene Resultat offenbar so aussprechen, daß ein solches System $\mathfrak{P}$ durch Aufnahme von beliebig vielen einfachen, durch $\mathfrak{a}$ theilbaren Moduln in ein ebenfalls vollständiges System $\mathfrak{R}$ übergeht, und daß beiden Systemen $\mathfrak{P}$ und $\mathfrak{R}$ ein und dasselbe Idealproduct u entspricht. Ist nun $\mathfrak{Q}$ ebenfalls ein vollständiges System, und bezeichnet man mit $\mathfrak{R}$ das aus $\mathfrak{P}$ und $\mathfrak{Q}$ zusammengesetzte System, welches aus $\mathfrak{P}$ durch Hinzufügung von $\mathfrak{Q}$, aus $\mathfrak{Q}$ durch Hinzufügung von $\mathfrak{P}$ entsteht, so leuchtet ein, daß auch den beiden Systemen $\mathfrak{P}$, $\mathfrak{Q}$ ein und dasselbe Idealproduct u entspricht, w. z. b. w.

Ist $\mathfrak{a}$ selbst ein einfacher Modul, so wird die Darstellung (17) durch $n = 1$, $\mathfrak{p}_1 = \mathfrak{a}$ erfüllt, d. h. $\mathfrak{a}$ selbst bildet ein vollständiges System, und das ihm entsprechende Idealproduct u reducirt sich auf den einzigen Factor $(\mathfrak{a}; \mathfrak{a} - \mathfrak{b})$, welcher nach (14) mit $(\mathfrak{a}; \mathfrak{b})$ identisch ist. Wir wollen daher, wenn $\mathfrak{a}$ und $\mathfrak{b}$ wieder beliebige Moduln bedeuten, welche der Bedingung $(\mathfrak{a}, \mathfrak{b}) > 1$ genügen, das invariante, von der Darstellung (17) gänzlich unabhängige Idealproduct u in (20) auch mit dem Symbol $(\mathfrak{a}; \mathfrak{b})$ bezeichnen; es wird daher

$$(30) \qquad (\mathfrak{a}; \mathfrak{b}) = (\mathfrak{p}_1; \mathfrak{a}_1)\,(\mathfrak{p}_2; \mathfrak{a}_2) \ldots (\mathfrak{p}_n; \mathfrak{a}_n),$$

wo $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_n$ einfache Moduln bedeuten, welche der Bedingung (17) genügen, während $\mathfrak{a}_1, \mathfrak{a}_2 \ldots \mathfrak{a}_n$ durch (18) oder (19) bestimmt sind; die Bedeutung jedes Factors von $(\mathfrak{a}; \mathfrak{b})$ ist früher in (11) erklärt. Zufolge (21) ist zugleich

$$(31) \qquad (\mathfrak{a}, \mathfrak{b}) = N(\mathfrak{a}; \mathfrak{b}).$$

Wir betrachten nun noch die beiden, bis jetzt ausgeschlossenen Fälle, wo $(\mathfrak{a}, \mathfrak{b}) = 1$ oder $= 0$ ist. Der erstere Fall tritt dann und nur dann ein, wenn $\mathfrak{a} > \mathfrak{b}$ ist (also immer für $\mathfrak{a} = 0$); soll

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

nun das Gesetz (31) bestehen bleiben, so müssen wir definiren

$$(32) \qquad (\mathfrak{a};\mathfrak{b}) = \mathfrak{z}, \text{ wenn } (\mathfrak{a},\mathfrak{b}) = 1.$$

Aber man kann auch (mit einziger Ausnahme des Falles $\mathfrak{a} = 0$) die Definition (30) anwenden; denn jedes beliebig ausgewählte System $\mathfrak{P}$ von einfachen, durch $\mathfrak{a}$ theilbaren Moduln $\mathfrak{p}_\nu$ ist im obigen Sinne ein vollständiges System, und da nach (15) jeder Factor $(\mathfrak{p}_\nu; \mathfrak{a}_\nu) = \mathfrak{z}$ wird, weil $\mathfrak{a}_\nu = \mathfrak{a}$ ist, so folgt aus (30) auch (32). Soll endlich das Gesetz (31) auch im zweiten Falle erhalten bleiben, so müssen wir definiren

$$(33) \qquad (\mathfrak{a};\mathfrak{b}) = 0, \text{ wenn } (\mathfrak{a},\mathfrak{b}) = 0,$$

und man überzeugt sich leicht, daß dies mit (13) und auch mit (30) verträglich ist, wenn in diesem Falle überhaupt eine Darstellung von der Form (17) existirt.

Die Wahl der Bezeichnung $(\mathfrak{a};\mathfrak{b})$, in welche freilich die nothwendige Beziehung auf den Körper Z oder das Ideal $\mathfrak{z}$ nicht aufgenommen ist, rechtfertigt sich zunächst dadurch, daß $(\mathfrak{a};\mathfrak{b})$, wenn Z der Körper R der rationalen Zahlen, also $\mathfrak{z}$ das System $\mathfrak{z}$ aller ganzen rationalen Zahlen ist, mit $(\mathfrak{a},\mathfrak{b})$ oder vielmehr mit dem eingliedrigen Modul $\mathfrak{z}(\mathfrak{a},\mathfrak{b})$ zusammenfällt; dies folgt unmittelbar aus (31) oder auch aus (11) und (30). Außerdem gelten aber für das neue Symbol $(\mathfrak{a};\mathfrak{b})$, wie wir jetzt beweisen wollen, auch dieselben Hauptsätze (D. S. 510, 511), wie für das alte Symbol $(\mathfrak{a},\mathfrak{b})$[1]).

§ 3.

Die Darstellung (17) und das daraus abgeleitete Idealproduct in (20) oder (30) bleibt offenbar ungeändert, wenn $\mathfrak{a}$ festgehalten, aber $\mathfrak{b}$ durch $\mathfrak{a}-\mathfrak{b}$ ersetzt wird; hieraus folgt unmittelbar der Satz

$$(34) \qquad (\mathfrak{a};\mathfrak{b}) = (\mathfrak{a};\mathfrak{a}-\mathfrak{b}).$$

Aus der Darstellung (17) folgt ferner durch Addition von $\mathfrak{b}$, weil $(\mathfrak{a}-\mathfrak{b})+\mathfrak{b} = \mathfrak{b} = (\mathfrak{a}+\mathfrak{b})-\mathfrak{b}$ ist, die Darstellung

$$\mathfrak{a}+\mathfrak{b} = \mathfrak{b}+\mathfrak{p}_1+\mathfrak{p}_2+\cdots+\mathfrak{p}_n,$$

welche für die beiden Moduln $\mathfrak{a}+\mathfrak{b}, \mathfrak{b}$ dieselbe Bedeutung hat, wie (17) für $\mathfrak{a}, \mathfrak{b}$; wir bilden daher, wie in (18), die entsprechende Kette

1) Vergl. auch § 6 der von H. Weber und mir verfaßten Abhandlung Theorie der algebraischen Functionen einer Veränderlichen (Crelle's Journal Bd. 92).

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

der Moduln

$$\mathfrak{a}'_{\nu-1} = \mathfrak{b} + \mathfrak{p}_\nu + \mathfrak{p}_{\nu+1} + \cdots + \mathfrak{p}_n, \quad \mathfrak{a}'_n = \mathfrak{b}$$

und erhalten nach (30) zunächst

$$(\mathfrak{a} + \mathfrak{b}; \mathfrak{b}) = (\mathfrak{p}_1; \mathfrak{a}'_1)(\mathfrak{p}_2; \mathfrak{a}'_2) \ldots (\mathfrak{p}_n; \mathfrak{a}'_n).$$

Zwischen den beiden Ketten der Moduln $\mathfrak{a}_\nu$ und $\mathfrak{a}'_\nu$ besteht nun die durch die beiden Gleichungen

$$\mathfrak{a}'_\nu = \mathfrak{b} + \mathfrak{a}_\nu, \quad \mathfrak{a}_\nu = \mathfrak{a} - \mathfrak{a}'_\nu$$

ausgedrückte Correspondenz (vergl. D. S. 499 Anm.); die erste ergiebt sich unmittelbar aus (18) durch Addition von $\mathfrak{b}$, und aus ihr folgt die zweite; da nämlich $\mathfrak{a}_\nu > \mathfrak{a}$ ist, so gilt nach einem Satze der allgemeinen Modultheorie (D. S. 498) die Gleichung

$$(\mathfrak{a} - \mathfrak{b}) + \mathfrak{a}_\nu = \mathfrak{a} - (\mathfrak{b} + \mathfrak{a}_\nu),$$

welche mit der zu beweisenden zusammenfällt, weil $\mathfrak{a} - \mathfrak{b} > \mathfrak{a}_\nu$ ist. Da ferner $\mathfrak{p}_\nu > \mathfrak{a}$ ist, so folgt hieraus weiter

$$\mathfrak{p}_\nu - \mathfrak{a}_\nu = \mathfrak{p}_\nu - \mathfrak{a} - \mathfrak{a}'_\nu = \mathfrak{p}_\nu - \mathfrak{a}'_\nu,$$

also nach (14) oder (34) auch

$$(\mathfrak{p}_\nu; \mathfrak{a}_\nu) = (\mathfrak{p}_\nu; \mathfrak{a}'_\nu),$$

und wir erhalten den Satz

$$(35) \qquad (\mathfrak{a}; \mathfrak{b}) = (\mathfrak{a} + \mathfrak{b}; \mathfrak{b}).$$

Aus der Darstellung (17) folgt ferner durch Multiplication mit einem beliebigen einfachen Modul $\mathfrak{p}$ und mit Rücksicht auf (7) die Darstellung

$$\mathfrak{a}\mathfrak{p} = (\mathfrak{a}\mathfrak{p} - \mathfrak{b}\mathfrak{p}) + \mathfrak{p}\mathfrak{p}_1 + \mathfrak{p}\mathfrak{p}_2 + \cdots + \mathfrak{p}\mathfrak{p}_n;$$

der Kette der Moduln $\mathfrak{a}_\nu$ entspricht jetzt die Kette der Moduln $\mathfrak{a}_\nu\mathfrak{p}$, und hieraus ergiebt sich mit Rücksicht auf (16) der Satz

$$(36) \qquad (\mathfrak{a}\mathfrak{p}; \mathfrak{b}\mathfrak{p}) = (\mathfrak{a}; \mathfrak{b}).$$

Da ferner $(\mathfrak{p}_\nu; \mathfrak{a}_\nu)\,\mathfrak{p}_\nu = \mathfrak{p}_\nu - \mathfrak{a}_\nu > \mathfrak{a}_\nu$, und auch $(\mathfrak{p}_\nu; \mathfrak{a}_\nu)\,\mathfrak{a}_\nu > \mathfrak{a}_\nu$ ist, weil $(\mathfrak{p}_\nu; \mathfrak{a}_\nu) > \mathfrak{e}$, so folgt aus (19) durch Multiplication mit $(\mathfrak{p}_\nu; \mathfrak{a}_\nu)$, daß auch $(\mathfrak{p}_\nu; \mathfrak{a}_\nu)\,\mathfrak{a}_{\nu-1} > \mathfrak{a}_\nu$, und da $\mathfrak{a}_0 = \mathfrak{a}$ und $\mathfrak{a}_n = \mathfrak{a} - \mathfrak{b}$, so ergiebt sich aus (30) der Satz

$$(37) \qquad (\mathfrak{a}; \mathfrak{b})\,\mathfrak{a} > \mathfrak{a} - \mathfrak{b}.$$

Ist endlich $\mathfrak{a} < \mathfrak{b}$, und $\mathfrak{b} < \mathfrak{c}$, so ergiebt sich auch leicht der Satz

$$(38) \qquad (\mathfrak{a}; \mathfrak{c}) = (\mathfrak{a}; \mathfrak{b})(\mathfrak{b}; \mathfrak{c}),$$

wenn man die Darstellung (17), in welcher $\mathfrak{a} - \mathfrak{b} = \mathfrak{b}$ ist, mit einer

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

Darstellung von der Form

$$\mathfrak{b} = \mathfrak{c} + \mathfrak{q}_1 + \mathfrak{q}_2 + \cdots + \mathfrak{q}_s$$

verbindet, wo $\mathfrak{q}_1, \mathfrak{q}_2 \ldots \mathfrak{q}_s$ einfache Moduln bedeuten.

Die Beweise aller vorstehenden Sätze (34) bis (38) stützen sich auf die Annahme der Existenz von solchen Darstellungen (17); aber man überzeugt sich mit Rücksicht auf (32) und (33) leicht, daß die Sätze auch dann gültig bleiben, wenn diese Annahme nicht erfüllt ist.

§ 4.

Wir wenden uns nun zu der Untersuchung der Beziehungen, welche zwischen unserem Symbole $(\mathfrak{a}; \mathfrak{b})$ und gewissen Determinanten bestehen und denjenigen ganz ähnlich sind, welche für das alte Symbol $(\mathfrak{a}, \mathfrak{b})$ gelten (D. S. 521—523).

Hierbei gehen wir, indem wir $(\mathfrak{a}, \mathfrak{b}) > 0$ voraussetzen, wieder von der Darstellung (17) des Moduls $\mathfrak{a}$ aus und betrachten jedes System L von n Zahlen $\pi_1, \pi_2 \ldots \pi_n$, welche resp. in $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_n$, also auch in $\mathfrak{a}$ enthalten sind und zugleich der Congruenz

$$\pi_1 + \pi_2 + \cdots + \pi_n \equiv 0 \pmod{\mathfrak{b}} \tag{39}$$

genügen. Aus je n solchen Lösungen $L', L'' \ldots L^{(n)}$ dieser Congruenz bilden wir, indem wir die in ihnen auftretenden Zahlen π_ν mit entsprechenden Accenten versehen, die Determinante

$$\lambda = \Sigma \pm \pi_1' \pi_2'' \ldots \pi_n^{(n)}, \tag{40}$$

welche offenbar, wie jedes ihrer Glieder, in dem einfachen Modul

$$\mathfrak{p} = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n \tag{41}$$

enthalten ist. Da $(\mathfrak{a}, \mathfrak{b})\,\mathfrak{a} > \mathfrak{b}$ ist (D. S. 511), und folglich, wenn α_ν eine willkürliche Zahl in $\mathfrak{p}_\nu$ bedeutet, die Zahl $\pi_\nu = (\mathfrak{a}, \mathfrak{b})\,\alpha_\nu$ für sich allein eine Lösung $L^{(\nu)}$ der Congruenz (39) bildet, während die übrigen Glieder verschwinden, so leuchtet ein, daß unter den Determinanten λ sich auch solche befinden, welche von Null verschieden sind. Da außerdem $z\lambda > \mathfrak{p}$ ist, so erzeugt (nach § 2. I) jede von Null verschiedene Determinante λ ein Ideal $\lambda\mathfrak{p}^{-1}$, und wir wollen beweisen, daß das Ideal $(\mathfrak{a}; \mathfrak{b})$ der größte gemeinsame Theiler aller dieser Ideale $\lambda\mathfrak{p}^{-1}$ ist, was wir in unseren Zeichen (D. S. 496) durch

$$(\mathfrak{a}; \mathfrak{b}) = \sum \lambda\mathfrak{p}^{-1} \text{ oder } (\mathfrak{a}; \mathfrak{b})\,\mathfrak{p} = \sum z\lambda \tag{42}$$

ausdrücken können.

Hierzu wenden wir die vollständige Induction an, indem wir die Darstellung (17) in die beiden folgenden

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

$$\mathfrak{a} = \mathfrak{a}_1 + \mathfrak{p}_1 \tag{43}$$

$$\mathfrak{a}_1 = (\mathfrak{a}-\mathfrak{b}) + \mathfrak{p}_2 + \mathfrak{p}_3 + \cdots + \mathfrak{p}_n \tag{44}$$

zerlegen, welche, weil $\mathfrak{a}-\mathfrak{a}_1 = \mathfrak{a}_1$ und $\mathfrak{a}_1-\mathfrak{b} = \mathfrak{a}-\mathfrak{b}$ ist, für die Modulpaare $\mathfrak{a}, \mathfrak{a}_1$ und $\mathfrak{a}_1, \mathfrak{b}$ dieselbe Bedeutung haben, wie die Darstellung (17) für das Modulpaar $\mathfrak{a}, \mathfrak{b}$; aus (30) folgt zugleich

$$(\mathfrak{a}; \mathfrak{b}) = (\mathfrak{p}_1; \mathfrak{a}_1)(\mathfrak{a}_1; \mathfrak{b}). \tag{45}$$

Unser Beweis setzt sich nun aus den folgenden fünf Hauptpuncten zusammen.

1. Betrachten wir zunächst, um den Fall $n = 1$ zu erledigen, nur das Modulpaar $\mathfrak{a}, \mathfrak{a}_1$, also die Darstellung (43), so sind nach (39) alle diejenigen in $\mathfrak{p}_1$ enthaltenen Zahlen π_1 zu bilden, welche der Congruenz $\pi_1 \equiv 0 \pmod{\mathfrak{a}_1}$ genügen, d. h. alle Zahlen π_1 des einfachen Moduls

$$\mathfrak{n} = \mathfrak{p}_1-\mathfrak{a}_1 = (\mathfrak{p}_1; \mathfrak{a}_1)\mathfrak{p}_1 = (\mathfrak{a}; \mathfrak{a}_1)\mathfrak{p}_1; \tag{46}$$

da nun jede aus einem einzigen Elemente π_1 gebildete Determinante ersten Grades $= \pi_1$ ist, und außerdem zufolge der Eigenschaft (2) j e d e r Modul

$$\mathfrak{n} = \sum \varepsilon\pi_1 \tag{47}$$

ist, wo π_1 alle Zahlen in $\mathfrak{n}$ durchläuft, so leuchtet für diesen Fall $n = 1$ die Richtigkeit des Satzes (42) ein.

2. Dem Verfahren des Inductionsbeweises gemäß nehmen wir jetzt an, unser Satz sei für das in der Darstellung (44) auftretende Modulpaar $\mathfrak{a}_1, \mathfrak{b}$ bewiesen, und wir haben zu zeigen, daß hieraus seine Richtigkeit auch für das Modulpaar $\mathfrak{a}, \mathfrak{b}$ folgt. Nach der obigen Vorschrift besteht diese Annahme im Folgenden. Man betrachte jedes System M von $(n-1)$ Zahlen $\varrho_2, \varrho_3 \ldots \varrho_n$, welche resp. in $\mathfrak{p}_2, \mathfrak{p}_3 \ldots \mathfrak{p}_n$ enthalten sind und zugleich der Congruenz

$$\varrho_2 + \varrho_3 + \cdots + \varrho_n \equiv 0 \pmod{\mathfrak{b}} \tag{48}$$

genügen; aus je $(n-1)$ solchen Lösungen M', $M'' \ldots M^{(m)}$ bilde man die Determinante

$$\mu = \sum \pm \varrho_2' \varrho_3'' \ldots \varrho_n^{(n)}, \tag{49}$$

so wird

$$(\mathfrak{a}_1; \mathfrak{b}) = \sum \mu q^{-1} \text{ oder } (\mathfrak{a}_1; \mathfrak{b})\mathfrak{q} = \sum \varepsilon\mu, \tag{50}$$

wo zur Abkürzung

$$\mathfrak{q} = \mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_n, \text{ also } \mathfrak{p} = \mathfrak{q}\mathfrak{p}_1 \tag{51}$$

gesetzt ist.

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

3. Wenden wir uns nun zu dem Modulpaare $\mathfrak{a}, \mathfrak{b}$, also zu der aus (43) und (44) zusammengesetzten Darstellung (17) und zu der ihr entsprechenden Congruenz (39), so bemerken wir vor allen Dingen, daß der Inbegriff aller in der letzteren auftretenden Zahlen π_1 identisch ist mit dem obigen Modul $\mathfrak{n}$ in (46). Da nämlich die Zahlen π_ν in $\mathfrak{p}_\nu$, also auch in $\mathfrak{a}$ enthalten sind, so gilt die auf den Modul $\mathfrak{b}$ bezügliche Congruenz (39) von selbst auch für den Modul $\mathfrak{a}-\mathfrak{b}$ und ist daher gleichbedeutend mit einer Gleichung von der Form

$$\pi_1 = \sigma - \pi_2 - \pi_3 - \cdots - \pi_n,$$

wo σ eine Zahl des Moduls $\mathfrak{a}-\mathfrak{b}$ bedeutet; hieraus geht aber mit Rücksicht auf (44) hervor, daß die in $\mathfrak{p}_1$ enthaltene Zahl π_1 auch in $\mathfrak{a}_1$, also auch in $\mathfrak{n} = \mathfrak{p}_1 - \mathfrak{a}_1$ enthalten ist; und da umgekehrt jede in $\mathfrak{n}$, also gleichzeitig in $\mathfrak{p}_1$ und $\mathfrak{a}_1$ enthaltene Zahl π_1 gewiß von der vorstehenden Form ist, aus welcher wieder die Congruenz (39) folgt, so ergiebt sich hieraus die oben behauptete Identität aller in der Congruenz (39) auftretenden Zahlen π_1 mit allen in 1. betrachteten Zahlen π_1 des Moduls $\mathfrak{n}$, und folglich gilt für diese Zahlen π_1 auch wieder die Gleichung (47).

4. Nun leuchtet ein, daß jede Lösung M der Congruenz (48) auch als eine Lösung L der Congruenz (39) aufgefaßt werden kann, in welcher $\pi_1 = 0$ ist. Combinirt man daher je $(n-1)$ Lösungen der Congruenz (48), denen die Determinante μ in (49) entspricht, mit jeder Lösung L der Congruenz (39), so entspricht diesem System von n Lösungen zufolge (40) eine Determinante $\lambda = \pi_1 \mu$. Unter den sämmtlichen Moduln $\varepsilon\lambda$ befinden sich daher auch alle Moduln von der Form $\varepsilon\pi_1 \cdot \varepsilon\mu$, und folglich ist der größte gemeinsame Theiler $\sum \varepsilon\lambda$ der ersteren auch ein Theiler der letzteren, also auch ihres größten gemeinsamen Theilers, und da der letztere, weil die Factoren π_1, μ gänzlich unabhängig von einander sind, von der Form

$$\sum \varepsilon\pi_1 \cdot \varepsilon\mu = \sum \varepsilon\pi_1 \cdot \sum \varepsilon\mu$$

ist, so ergiebt sich zufolge (47) das Resultat

$$\sum \varepsilon\lambda < \mathfrak{n} \sum \varepsilon\mu,$$

welches mit Rücksicht auf (45), (46), (50), (51) die Form

$$\sum \lambda\mathfrak{p}^{-1} < (\mathfrak{a}; \mathfrak{b}) \tag{52}$$

annimmt.

5. Schwieriger ist der Beweis, daß das Ideal linker Hand auch durch das zur Rechten theilbar ist. Nach einer früheren Bemerkung (§ 2. I) kann man aus dem einfachen Modul $\mathfrak{n}$ eine Zahl ω_1 so auswählen, daß $u = \omega_1 \mathfrak{n}^{-1}$ relatives Primideal zu $(\mathfrak{a}; \mathfrak{b})$ wird,

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

und hierauf kann man aus u eine Zahl a wählen, welche relative Primzahl zu $(\mathfrak{a}; \mathfrak{b})$ ist, weil jedes Ideal u sich durch Multiplication mit einem Ideal v, welches relatives Primideal zu $(\mathfrak{a}; \mathfrak{b})$ ist, in ein Hauptideal $za = uv$ verwandeln läßt (D. S. 559); zugleich wird $a\mathfrak{n} = v\omega_1 > z\omega_1$, und folglich wird jede Zahl π_1 des Moduls $\mathfrak{n}$ durch Multiplication mit a in eine Zahl

$$a\pi_1 = c\omega_1 \tag{53}$$

verwandelt, wo c ebenso wie a in z enthalten ist. Da ferner ω_1 eine Zahl in $\mathfrak{n}$ ist, so giebt es zufolge 3. in den Moduln $\mathfrak{p}_2, \mathfrak{p}_3 \ldots \mathfrak{p}_n$ resp. Zahlen $\omega_2, \omega_3 \ldots \omega_n$, welche die Congruenz

$$\omega_1 + \omega_2 + \omega_3 + \cdots + \omega_n \equiv 0 \pmod{\mathfrak{b}} \tag{54}$$

erfüllen, also mit ω_1 eine particuläre Lösung der Congruenz (39) bilden. Betrachtet man nun jede Lösung L der letzteren, bestimmt aus der in ihr enthaltenen Zahl π_1 gemäß (53) die zugehörige ganze Zahl c und setzt

$$\varrho_\nu = a\pi_\nu - c\omega_\nu, \tag{55}$$

so ist $\varrho_1 = 0$, und die $n-1$ Zahlen $\varrho_2, \varrho_3 \ldots \varrho_n$, welche resp. in $\mathfrak{p}_2, \mathfrak{p}_3 \ldots \mathfrak{p}_n$ enthalten sind, bilden, wie sich durch Multiplication der Congruenzen (39), (54) mit den ganzen Zahlen a, c und Subtraction ergiebt, eine Lösung M der Congruenz (48). Betrachtet man nun wieder je n Lösungen $L', L'' \ldots L^{(n)}$ der Congruenz (39), welche die Determinante λ in (40) erzeugen, und versieht die nach (53) und (55) daraus abgeleiteten Zahlen c und Lösungen M mit entsprechenden Accenten, so ist nach bekannten Sätzen

$$a^n\lambda = \begin{vmatrix} c'\omega_1, & a\pi_2' \ldots a\pi_n' \\ c''\omega_1, & a\pi_2'' \ldots a\pi_n'' \\ \cdots & \cdots \\ c^{(n)}\omega_1, & a\pi_2^{(n)} \ldots a\pi_n^{(n)} \end{vmatrix} = \begin{vmatrix} a\pi_1', & \varrho_2' \ldots \varrho_n' \\ a\pi_1'', & \varrho_2'' \ldots \varrho_n'' \\ \cdots & \cdots \\ a\pi_1^{(n)}, & \varrho_2^{(n)} \ldots \varrho_n^{(n)} \end{vmatrix}$$

$$= a(\pi_1'\mu' + \pi_1''\mu'' + \cdots + \pi_1^{(n)}\mu^{(n)}),$$

wo $\mu', \mu'' \ldots \mu^{(n)}$ Determinanten μ von der Form (49) bedeuten, also zufolge (50) in $(\mathfrak{a}_1; \mathfrak{b})\mathfrak{q}$ enthalten sind; da ferner die Factoren π_1 in $\mathfrak{n} = (\mathfrak{p}_1; \mathfrak{a}_1)\mathfrak{p}_1$, also die Producte $\pi_1\mu$ und $a\pi_1\mu$ zufolge (45), (51) in $(\mathfrak{a}; \mathfrak{b})\mathfrak{p}$ enthalten sind, so ergiebt sich aus der vorstehenden Gleichung zunächst $a^n\lambda\mathfrak{p}^{-1} > (\mathfrak{a}; \mathfrak{b})$ und folglich, weil a^n wie a relative Primzahl zu $(\mathfrak{a}; \mathfrak{b})$ ist, auch $\lambda\mathfrak{p}^{-1} > (\mathfrak{a}; \mathfrak{b})$, mithin auch

$$\sum \lambda\mathfrak{p}^{-1} > (\mathfrak{a}; \mathfrak{b}), \tag{56}$$

woraus mit Rücksicht auf (52) der Satz (42) folgt, w. z. b. w. —

Dieser Satz kommt nun meistens in der Weise zur Anwendung,

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

daß die in der Darstellung (17) auftretenden einfachen Moduln $\mathfrak{p}_\nu$ gemäß (5) in der Form

(57) $$\mathfrak{p}_\nu = x_\nu \alpha_\nu$$

ausgedrückt sind, wo x_ν einen Idealbruch, α_ν eine von Null verschiedene Zahl bedeutet, und hiermit nimmt die Darstellung (17) folgende Form an:

(58) $$\mathfrak{a} = (\mathfrak{a}-\mathfrak{b}) + x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n.$$

Zugleich geht die Congruenz (39), wenn man $\pi_\nu = a_\nu \alpha_\nu$ setzt, in

(59) $$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \equiv 0 \pmod{\mathfrak{b}}$$

über, wo $a_1, a_2 \ldots a_n$ Zahlen bedeuten, welche resp. in den Idealbrüchen $x_1, x_2 \ldots x_n$ enthalten sind. Bildet man nun aus je n solchen, durch Accente unterschiedenen Lösungen der Congruenz (59) die Determinante

(60) $$A = \sum \pm a_1' a_2'' \ldots a_n^{(n)}$$

und setzt zur Abkürzung

(61) $$X = x_1 x_2 \ldots x_n,$$

so nimmt unser Satz (42) mit Rücksicht auf (40) und (41) die Form

(62) $$(\mathfrak{a}; \mathfrak{b})\, X = \sum \varepsilon A$$

an, in welcher nur Zahlen und Idealbrüche des Körpers Z auftreten. —

Bevor wir weiter gehen, wollen wir bemerken, daß der Satz (42) offenbar auch als Definition des Symbols $(\mathfrak{a}; \mathfrak{b})$ dienen könnte. Da die Ideale $\lambda\mathfrak{p}^{-1}$ von der Reihenfolge der einfachen Moduln $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_n$ im Systeme $\mathfrak{P}$ gänzlich unabhängig sind, so besitzt diese Definition vor der früheren (in § 2) den Vorzug, daß die Invarianz leichter nachweisbar ist; denn durch Betrachtungen, welche den bei dem obigen Beweise angewendeten ganz ähnlich sind, ergiebt sich sofort, daß der größte gemeinsame Theiler aller dem Systeme $\mathfrak{P}$ entsprechenden Ideale $\lambda\mathfrak{p}^{-1}$ sich nicht ändert, wenn zu $\mathfrak{P}$ noch irgend ein durch $\mathfrak{a}$ theilbarer einfacher Modul hinzugefügt wird, und hieraus folgt wie früher (§ 2), daß dieser größte gemeinsame Theiler auch von der Auswahl des vollständigen Systemes $\mathfrak{P}$ unabhängig ist. Auch kann man offenbar der Definition schon vor diesem Nachweise die völlige Invarianz verleihen, wenn man $(\mathfrak{a}; \mathfrak{b})$ als den größten gemeinsamen Theiler aller Ideale $\lambda\mathfrak{p}^{-1}$ erklärt, welche allen vollständigen Systemen $\mathfrak{P}$ entsprechen.

Unsere frühere Definition von $(\mathfrak{a}; \mathfrak{b})$ hat dagegen den Vorzug, daß sie der Determinanten λ gar nicht bedarf und sich nur auf

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

die Bildung von Moduln stützt; will man ihr ferner von vornherein den Charakter der Invarianz verleihen, so wird man wieder (a; b) als den größten gemeinsamen Theiler aller Producte

$$\frac{\mathfrak{p}_1 - \mathfrak{a}_1}{\mathfrak{p}_1} \cdot \frac{\mathfrak{p}_2 - \mathfrak{a}_2}{\mathfrak{p}_2} \cdots \frac{\mathfrak{p}_n - \mathfrak{a}_n}{\mathfrak{p}_n}$$

erklären, die allen zur Darstellung (17) tauglichen Folgen von einfachen Moduln $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_n$ entsprechen. Immerhin bleibt die eine wie die andere Definition von (a; b) hinsichtlich ihrer Einfachheit außerordentlich weit zurück hinter der Definition des alten Symbols (a, b), welche sich unmittelbar auf die Betrachtung der in den Moduln a, b enthaltenen Zahlen stützt (D. S. 509). Nachdem ich seit vielen Jahren eine ähnliche Vereinfachung vergeblich gesucht habe, kann ich nur noch den Wunsch aussprechen, daß es einem Anderen gelingen möge, eine solche zu finden.

§ 5.

Wir wenden uns jetzt zu denjenigen Sätzen, welche vorzugsweise von endlichen Moduln handeln. Hierbei werden wir öfter den der allgemeinen Modultheorie angehörenden Satz

$$(\varrho + \sigma)\,\mathfrak{m} > \varrho\mathfrak{m} + \sigma\mathfrak{m} \tag{63}$$

anzuwenden haben, welcher offenbar für je zwei Zahlen ϱ, σ und jeden Modul $\mathfrak{m}$ gilt; denn wenn μ jede Zahl des Moduls $\mathfrak{m}$ bedeutet, so ist jede Zahl des Moduls linker Hand von der Form $(\varrho + \sigma)\mu = \varrho\mu + \sigma\mu$, also auch in dem Modul rechter Hand enthalten[1]); auch leuchtet ein, daß derselbe Satz für Summen von beliebig vielen Gliedern gilt. Nach dieser Vorbemerkung stellen wir den folgenden Satz auf, welcher die Grundlage für unsere Untersuchung bildet (vergl. D. S. 516).

I. Ist der letzte der drei Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ einfach, so kann man

$$(\mathfrak{c} + \mathfrak{a}) - \mathfrak{b} = \mathfrak{q} + (\mathfrak{a} - \mathfrak{b}) \tag{64}$$

setzen, wo $\mathfrak{q}$ ein einfacher Modul oder $= 0$ ist.

Um dies zu beweisen, setzen wir zur Abkürzung[2])

1) Vergl. D. S. 501, wo dieser fast selbstverständliche Satz doch hätte erwähnt werden sollen.

2) Diese Bezeichnung der Moduln durch Accente und Indices entnehme ich einer noch nicht veröffentlichten Arbeit über die aus drei beliebigen Moduln $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ entspringende Gruppe von 28 Moduln, welche sich in neun verschiedene Stufen vertheilen (vergl. D. Anm. auf S. 499, 510).

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

$$\mathfrak{a}'' = (\mathfrak{c}+\mathfrak{a})-(\mathfrak{a}+\mathfrak{b}) \tag{65}$$

$$\mathfrak{b}_1 = \mathfrak{a}''-\mathfrak{b} = (\mathfrak{c}+\mathfrak{a})-\mathfrak{b} \tag{66}$$

$$\mathfrak{c}_1 = \mathfrak{a}''-\mathfrak{c} = \mathfrak{c}-(\mathfrak{a}+\mathfrak{b}). \tag{67}$$

Nach einem Satze der allgemeinen Modultheorie (D. S. 499) ist dann

$$\mathfrak{a}'' = \mathfrak{c}_1+\mathfrak{a} = \mathfrak{b}_1+\mathfrak{a}, \tag{68}$$

und die zu beweisende Gleichung (64) lautet

$$\mathfrak{b}_1 = \mathfrak{q}+(\mathfrak{a}-\mathfrak{b}). \tag{69}$$

Wir bemerken nun zunächst, daß es immer zwei Zahlen ϱ, σ giebt, welche den drei Bedingungen

$$\varrho+\sigma = 1,\ \varrho\mathfrak{c}_1 > \mathfrak{b}_1,\ \sigma\mathfrak{c}_1 > \mathfrak{a} \tag{70}$$

genügen; dies leuchtet unmittelbar ein, falls $\mathfrak{c}_1 = 0$ ist, weil dann die beiden letzten Bedingungen von selbst erfüllt sind; im entgegengesetzten Falle ist $\mathfrak{c}_1$ (nach § 2. I) als Vielfaches von $\mathfrak{c}$ ebenfalls einfach, und da aus (68) sich $\mathfrak{c}_1 > \mathfrak{b}_1+\mathfrak{a}$, also $\mathfrak{z} > \mathfrak{b}_1\mathfrak{c}_1^{-1}+\mathfrak{a}\mathfrak{c}_1^{-1}$ ergiebt, so kann man die in $\mathfrak{z}$ enthaltene Zahl $1 = \varrho+\sigma$ setzen, wo die Zahlen ϱ, σ resp. in $\mathfrak{b}_1\mathfrak{c}_1^{-1}$, $\mathfrak{a}\mathfrak{c}_1^{-1}$ enthalten sind und folglich den Bedingungen (70) genügen. Wie nun auch diese Zahlen übrigens gewählt sein mögen, so ergiebt sich leicht, daß der Modul

$$\mathfrak{q} = \varrho\mathfrak{c}_1, \tag{71}$$

welcher offenbar einfach oder $= 0$ ist, unserem Satze (69) genügt. Wendet man nämlich den Hüfssatz (63) auf den Fall $\mathfrak{m} = \mathfrak{c}_1$ an mit Rücksicht auf (70), so folgt $\mathfrak{c}_1 > \mathfrak{q}+\mathfrak{a}$, und da zufolge (70) auch $\mathfrak{q} > \mathfrak{b}_1$ ist, so ergiebt sich aus (68), daß

$$\mathfrak{a}'' = \mathfrak{c}_1+\mathfrak{a} > \mathfrak{q}+\mathfrak{a} > \mathfrak{b}_1+\mathfrak{a} = \mathfrak{a}'',$$

also

$$\mathfrak{a}'' = \mathfrak{q}+\mathfrak{a},$$

und folglich nach (66)

$$\mathfrak{b}_1 = \mathfrak{a}''-\mathfrak{b} = (\mathfrak{q}+\mathfrak{a})-\mathfrak{b}$$

ist; bedenkt man aber, daß $\mathfrak{q} > \mathfrak{b}_1 > \mathfrak{b}$ ist, so folgt hieraus nach einem Satze der allgemeinen Modultheorie (D. S. 498) auch die Gleichung (69), w. z. b. w. Hieraus folgt unmittelbar der Satz

II. Jedes Vielfache einer Summe von n einfachen Moduln ist darstellbar als Summe von höchstens n einfachen Moduln.

Dies ist nämlich für den Fall $n = 1$ schon früher (§ 2. I) bewiesen, und wenn der Satz für jedes Vielfache $\mathfrak{a}-\mathfrak{b}$ einer Summe $\mathfrak{a}$

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

von n einfachen Moduln gilt, so gilt er nach dem vorhergehenden Satze auch für jedes Vielfache $(c + a) - b$ einer Summe $c + a$ von $(n + 1)$ einfachen Moduln, also allgemein, w. z. b. w.

Es verlohnt sich aber der Mühe, nach den Vorschriften des vorhergehenden Satzes die Form irgend eines Vielfachen $a - b$ einer Summe

$$a = \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_n \tag{72}$$

von n einfachen Moduln $\mathfrak{p}_\nu$ wirklich herzustellen. Da immer $a = a + (a - b)$ ist, so können wir die in unserer früheren Untersuchung (§ 2) benutzten Bezeichnungen (17), (18) auch auf unseren Fall anwenden; setzen wir außerdem zur Abkürzung

$$\mathfrak{a}'_{\nu-1} = \mathfrak{p}_\nu + \mathfrak{p}_{\nu+1} + \cdots + \mathfrak{p}_n = \mathfrak{p}_\nu + \mathfrak{a}'_\nu, \quad \mathfrak{a}'_0 = a, \quad \mathfrak{a}'_n = 0, \tag{73}$$

so wird (zufolge D. S. 498), weil $\mathfrak{a}'_\nu > a$ ist,

$$\mathfrak{a}_\nu = (a - b) + \mathfrak{a}'_\nu = a - (b + \mathfrak{a}'_\nu), \quad \mathfrak{a}_\nu + b = b + \mathfrak{a}'_\nu,$$

also, weil $\mathfrak{p}_\nu > a$ ist,

$$\mathfrak{p}_\nu - \mathfrak{a}_\nu = \mathfrak{p}_\nu - (b + \mathfrak{a}'_\nu) = \mathfrak{p}_\nu - (\mathfrak{a}_\nu + b).$$

Ersetzen wir daher die in dem vorhergehenden Satz I und seinem Beweise auftretenden Moduln und Zahlen $\mathfrak{a}, \mathfrak{c}, \mathfrak{q}, \varrho, \sigma$ resp. durch $\mathfrak{a}'_\nu, \mathfrak{p}_\nu, \mathfrak{q}_\nu, \varrho_\nu, \sigma_\nu$, so wird zufolge (66), (67), (70)

$$\mathfrak{b}_1 = \mathfrak{a}'_{\nu-1} - b, \quad \mathfrak{c}_1 = \mathfrak{p}_\nu - \mathfrak{a}_\nu = (\mathfrak{p}_\nu; \mathfrak{a}_\nu)\,\mathfrak{p}_\nu \tag{74}$$

$$\varrho_\nu + \sigma_\nu = 1, \quad \mathfrak{q}_\nu = \varrho_\nu \mathfrak{c}_1 > \mathfrak{b}_1, \quad \sigma_\nu \mathfrak{c}_1 > \mathfrak{a}'_\nu \tag{75}$$

und zufolge (69) erhält man

$$\mathfrak{a}'_{\nu-1} - b = \mathfrak{q}_\nu + (\mathfrak{a}'_\nu - b),$$

woraus, weil $\mathfrak{a}'_n - b = 0$ ist, die Darstellung

$$a - b = \mathfrak{q}_1 + \mathfrak{q}_2 + \cdots + \mathfrak{q}_n \tag{76}$$

folgt.

Nehmen wir ferner an, die einfachen Moduln $\mathfrak{p}_\nu$ seien nach (5) in der Form

$$\mathfrak{p}_\nu = x_\nu \alpha_\nu \tag{77}$$

gegeben, wo x_ν einen Idealbruch und α_ν eine von Null verschiedene Zahl bedeutet, so kann man immer eine Zahl $c_\nu^{(\nu)}$ des Körpers Z und einen Idealbruch y_ν so wählen, daß

$$y_\nu c_\nu^{(\nu)} = (\mathfrak{p}_\nu; \mathfrak{a}_\nu)\, x_\nu, \tag{78}$$

also zufolge (74), (77)

$$\mathfrak{c}_1 = y_\nu c_\nu^{(\nu)} \alpha_\nu \tag{79}$$

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

wird; ist nämlich $(\mathfrak{p}_\nu; \mathfrak{a}_\nu)$ von Null verschieden, so kann man z. B. $c_\nu^{(\nu)} = 1$ setzen, während im Falle $(\mathfrak{p}_\nu; \mathfrak{a}_\nu) = 0$ auch $c_\nu^{(\nu)} = 0$ wird, y_ν aber willkürlich, z. B. $= z$ gewählt werden kann. Ist nun irgend eine Wahl von $c_\nu^{(\nu)}$ und y_ν getroffen, und setzt man mit Rücksicht auf (75)

$$\beta_\nu = c_\nu^{(\nu)} \alpha_\nu \varrho = c_\nu^{(\nu)} \alpha_\nu - c_\nu^{(\nu)} \alpha_\nu \sigma , \tag{80}$$

so wird

$$\mathfrak{q}_\nu = \varrho_\nu \mathfrak{c}_1 = y_\nu \beta_\nu . \tag{81}$$

Da nach (75) ferner $\sigma_\nu \mathfrak{c}_1 > \mathfrak{a}'_\nu$, also nach (79), (73), (77)

$$y_\nu c_\nu^{(\nu)} \alpha_\nu \sigma_\nu > x_{\nu+1} \alpha_{\nu+1} + \cdots + x_n \alpha_n ,$$

mithin

$$z c_\nu^{(\nu)} \alpha_\nu \sigma_\nu > y_\nu^{-1} x_{\nu+1} \alpha_{\nu+1} + \cdots + y_\nu^{-1} x_n \alpha_n$$

ist, so kann man die Zahl

$$- c_\nu^{(\nu)} \alpha_\nu \sigma_\nu = c_{\nu+1}^{(\nu)} \alpha_{\nu+1} + \cdots + c_n^{(\nu)} \alpha_n$$

und folglich nach (80)

$$\beta_\nu = c_\nu^{(\nu)} \alpha_\nu + c_{\nu+1}^{(\nu)} \alpha_{\nu+1} + \cdots + c_n^{(\nu)} \alpha_n \tag{82}$$

setzen, wo die Zahlen $c_\mu^{(\nu)}$ in $y_\nu^{-1} x_\mu$ enthalten sind, also den Bedingungen

$$y_\nu c_\mu^{(\nu)} > x_\mu \tag{83}$$

genügen, was zufolge (78) auch für den Fall $\mu = \nu$ gilt. Bildet man endlich das Product der n Gleichungen (78), und setzt zur Abkürzung

$$X = x_1 x_2 \ldots x_n , \quad Y = y_1 y_2 \ldots y_n \tag{84}$$

$$C = c_1' c_2'' \ldots c_n^{(n)} , \tag{85}$$

so ergiebt sich zufolge (30) der in allen Fällen gültige Satz

$$(\mathfrak{a}; \mathfrak{b})\ X = Y C , \tag{86}$$

und die Gleichungen (72), (76) gehen zufolge (77), (81) in

$$\mathfrak{a} = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n \tag{87}$$

$$\mathfrak{a} - \mathfrak{b} = y_1 \beta_1 + y_2 \beta_2 + \cdots + y_n \beta . \tag{88}$$

über.

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

Zur Erläuterung bemerken wir noch, daß die in den Gleichungen (81), (82), (83) enthaltene Darstellung von q_ν sich zwar einfacher schon aus der einen Bedingung $q_\nu > b_1 = a'_{\nu-1} - b$ in (75) ergiebt: aber hieraus würde auch mit Zuziehung der beiden anderen Bedingungen (75) die wichtige Beziehung (78), also auch der Satz (86) nicht nachträglich gefolgert werden können, wenigstens nicht ohne die neu hinzutretende Voraussetzung, daß das System der n Zahlen α_ν in Bezug auf den Körper Z irreducibel ist (D. S. 466). Diese Bemerkung möge zugleich den Uebergang bilden zu dem folgenden Fundamentalsatze (vergl. D. S. 518):

III. Wenn aus dem endlichen Modul a sich n und nicht mehr Zahlen so auswählen lassen, daß sie ein nach Z irreducibeles System bilden, so ist a darstellbar als Summe von n einfachen Moduln.

Um dies zu beweisen, wählen wir aus a ein nach Z irreducibeles System von n Zahlen $\alpha_1, \alpha_2 \ldots \alpha_n$; dann ist jede beliebige Zahl α in a von der Form

$$\alpha = h_1\alpha_1 + h_2\alpha_2 + \cdots + h_n\alpha_n,$$

wo die Coefficienten h_ν Zahlen des Körpers Z bedeuten (D. S. 467). Da ferner a ein endlicher Modul, also von der Form

$$a = [\alpha'_1, \alpha'_2 \ldots \alpha'_m]$$

ist (D. S. 494), so kann man, nachdem jede der m Basiszahlen α'_μ in der eben angegebenen Form

$$\alpha'_\mu = h_1^{(\mu)}\alpha_1 + h_2^{(\mu)}\alpha_2 + \cdots + h_n^{(\mu)}\alpha_n$$

dargestellt ist, bekanntlich eine von Null verschiedene Zahl a so wählen, daß alle mn Producte $ah_\nu^{(\mu)}$ ganze Zahlen des Körpers Z, also in z enthalten sind. Setzt man nun $\alpha_\nu = a\omega_\nu$ und

$$o = z\omega_1 + z\omega_2 + \cdots + z\omega_n,$$

so leuchtet ein, daß die m Basiszahlen α'_μ in o enthalten sind; mithin ist a theilbar durch o, und da o eine Summe von n einfachen Moduln ist, so gilt (nach dem vorhergehenden Satze II) dasselbe auch von a, w. z. b. w.

Es braucht kaum bemerkt zu werden, daß a auch nicht als Summe von weniger als n einfachen Moduln darstellbar ist, weil sonst je n Zahlen in a ein nach Z reducibeles System bilden würden (D. S. 468). Wir schließen unsere Untersuchung mit dem Beweise des folgenden Satzes (vergl. D. S. 521—523):

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

IV. Sind die beiden endlichen Moduln $\mathfrak{a}$, $\mathfrak{b}$, als Summen von einfachen Moduln in der Form

$$\mathfrak{a} = \sum^{\nu} x_\nu \alpha_\nu = x_1\alpha_1 + \cdots + x_n\alpha_n \tag{89}$$

$$\mathfrak{b} = \sum^{\mu} y_\mu \beta_\mu = y_1\beta_1 + \cdots + y_m\beta_m \tag{90}$$

dargestellt, wo x_ν, y_μ Idealbrüche, α_ν, β_μ von Null verschiedene Zahlen bedeuten, so bestehen die erforderlichen und hinreichenden Bedingungen für die Theilbarkeit

$$\mathfrak{b} > \mathfrak{a} \tag{91}$$

in m Gleichungen von der Form

$$\beta_\mu = \sum^{\nu} c_{\mu,\nu}\alpha_\nu = c_{\mu,1}\alpha_1 + \cdots + c_{\mu,n}\alpha_n, \tag{92}$$

wo die mn Zahlen $c_{\mu,\nu}$ den Bedingungen

$$y_\mu c_{\mu,\nu} > x_\nu \tag{93}$$

genügen. Ist ferner das System der n Zahlen α_ν irreducibel nach Z, und setzt man

$$X = x_1 x_2 \ldots x_n, \tag{94}$$

so wird

$$(\mathfrak{a};\ \mathfrak{b})\ X = \sum Y_\sigma C_\sigma, \tag{95}$$

wo die Modul-Summe auf alle Combinationen σ von je n Zahlen $\mu = 1', 2' \ldots n'$ aus der Reihe $1, 2 \ldots m$ zu erstrecken, und entsprechend

$$Y_\sigma = y_{1'} y_{2'} \cdots y_{n'} \tag{96}$$

$$C_\sigma = \sum \pm c_{1',1} c_{2',2} \cdots c_{n',n} \tag{97}$$

gesetzt ist.

Der erste Theil dieses Satzes ist leicht zu beweisen. Soll nämlich die Theilbarkeit (91) gelten, so muß auch $y_\mu\beta_\mu > \mathfrak{a}$, also

$$z\beta_\mu > \mathfrak{a}y_\mu^{-1} = \sum^{\nu} y_\mu^{-1} x_\nu \alpha_\nu$$

sein, und hieraus folgt die Existenz von Zahlen $c_{\mu,\nu}$, welche den Bedingungen (92), (93) genügen; und umgekehrt, wenn dieselben erfüllt sind, so folgt aus dem Hülfssatze (63), daß

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

$$y_\mu \beta_\mu = y_\mu \sum^{\nu} c_{\mu,\nu}\, \alpha_\nu > \sum^{\nu} y_\mu\, c_{\mu,\nu}\, \alpha_\nu > \sum^{\nu} x_\nu \alpha_\nu = \mathfrak{a},$$

also auch $\mathfrak{b} > \mathfrak{a}$ ist, was zu zeigen war. Den Beweis des zweiten Theiles kann man auf verschiedene Art führen; entweder transformirt man (nach II) den Modul $\mathfrak{b}$ in eine Summe von höchstens n einfachen Moduln und benutzt den dort bewiesenen Satz (86), oder man stützt sich unmittelbar auf den in § 4 enthaltenen Determinanten-Satz (62). Indem wir die Durchführung der ersteren Beweisart dem Leser überlassen (vergl. D. S. 519—523), wenden wir uns sofort zu der letzteren und betrachten alle Lösungen L der mit (59) übereinstimmenden Congruenz

$$(98) \qquad a_1 \alpha_1 + a_2 \alpha_2 + \cdots + a_n \alpha_n \equiv 0 \pmod{\mathfrak{b}}$$

durch n Zahlen a_ν, welche resp. den Idealbrüchen x_ν angehören. Nun ist zufolge (90) diese Congruenz gleichbedeutend mit der Existenz von m Zahlen b_μ, welche resp. in den Idealbrüchen y_μ enthalten sind und der Gleichung

$$(99) \qquad \sum^{\nu} a_\nu \alpha_\nu = \sum^{\mu} b_\mu \beta_\mu$$

genügen, und diese zerfällt zufolge (92) und vermöge der Irreducibilität des Systems der n Zahlen α_ν in n Gleichungen von der Form

$$(100) \qquad a_\nu = \sum^{\mu} b_\mu c_{\mu,\nu};$$

und umgekehrt folgt aus (92), (93), (90), daß jedes beliebige System von m aus den Idealbrüchen y_μ gewählten Zahlen b_μ vermöge (100) ein System von n Zahlen a_ν erzeugt, welche resp. den Idealbrüchen x_ν angehören und zugleich eine Lösung L der Congruenz (98) bilden. Betrachtet man nun (wie in § 4) irgend ein System von n solchen Lösungen $L', L'' \ldots L^{(n)}$, die wir ebenso wie die zugehörigen Zahlen a_ν, b_μ durch Accente unterscheiden, so folgt aus (100), daß die aus den n^2 Zahlen $a_\nu^{(\nu)}$ gebildete Determinante

$$(101) \qquad A = \sum^{\sigma} B_\sigma C_\sigma$$

ist, wo die Summe sich über alle im Satze genannten Combinationen σ erstreckt, und jede Determinante B_σ auf dieselbe Weise aus den Zahlen $b_\mu^{(\nu)}$ gebildet ist, wie C_σ aus den Zahlen $c_{\mu,\nu}$ in (97). Da nun jede Zahl $b_\mu^{(\nu)}$ in y_μ enthalten ist, so ist jedes Glied der Determinante B_σ und folglich diese selbst in dem Producte Y_σ enthalten, welches in (96) erklärt ist, also $zB_\sigma > Y_\sigma$, mithin

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

ergiebt sich aus (101) mit Rücksicht auf den Hülfssatz (63)

$$(102) \qquad zA > \sum^{\sigma} zB_\sigma C_\sigma > \sum^{\sigma} Y_\sigma C_\sigma,$$

also zufolge (62) auch

$$(103) \qquad (\mathfrak{a}; \mathfrak{b})\ X > \sum^{\sigma} Y_\sigma C_\sigma.$$

Wenn alle Determinanten C_σ verschwinden (wohin auch der Fall $m < n$ gehört), so bilden bekanntlich (D. S. 469) je n der m Zahlen β_μ in (92) und folglich auch je n Zahlen des Moduls $\mathfrak{b}$ in (90) ein nach Z reducibeles System; da aber allgemein $(\mathfrak{a}, \mathfrak{b})\ \mathfrak{a} > \mathfrak{b}$ ist (D. S. 511), so muß in diesem Falle gewiß $(\mathfrak{a}, \mathfrak{b}) = 0$ sein, weil sonst irgend ein in $\mathfrak{a}$ enthaltenes irreducibeles System von n Zahlen α'_ν, wie es zufolge (89) gewiß existirt, durch Multiplication mit $(\mathfrak{a}, \mathfrak{b})$ in ein ebenfalls irreducibeles System von n Zahlen in $\mathfrak{b}$ verwandelt würde; mithin ist zufolge (33) auch $(\mathfrak{a}; \mathfrak{b}) = 0$. Dies folgt aber auch unmittelbar aus (103), und unser Satz (95) ist also in diesem Falle richtig.

Wenn aber die Determinanten C_σ nicht alle verschwinden, so ist die in Z enthaltene Modul-Summe

$$(104) \qquad e = \sum^{\sigma} Y_\sigma C_\sigma$$

auch von Null verschieden, also (nach § 1) ein Idealbruch, und zufolge (102) ist Ae^{-1} stets (falls A nicht verschwindet) ein Ideal. Bedeutet nun p irgend ein gegebenes Primideal, so folgt aus

$$\sum^{\sigma} Y_\sigma C_\sigma e^{-1} = z,$$

daß es mindestens eine Combination σ giebt — sie mag aus den n ersten Indices $\nu = 1, 2 \ldots n$ bestehen — für welche das zugehörige Ideal $Y_\sigma C_\sigma e^{-1}$ nicht durch p theilbar ist. Für jeden solchen Index ν bilden wir nun nach (100) eine Lösung $L^{(\nu)}$ der Congruenz (98), indem wir die sämmtlichen m Zahlen $b_\mu = 0$ setzen mit einziger Ausnahme der Zahl b_ν, für welche wir eine noch näher zu bestimmende Zahl $b_\nu^{(\nu)}$ des Idealbruchs y_ν wählen; dieses System von m Zahlen b_μ erzeugt nach (100) eine aus den n Zahlen

$$a_1^{(\nu)} = b_\nu^{(\nu)} c_{\nu,1}, \quad a_2^{(\nu)} = b_\nu\ c_{\nu,2} \ldots a_n^{(\nu)} = b_\nu^{(\nu)} c_{\nu,n}$$

bestehende Lösung $L^{(\nu)}$ der Congruenz (98), und wenn man ebenso mit jedem der n Indices $1, 2 \ldots n$ der Combination σ verfährt, so erhält man n Lösungen $L', L'' \ldots L^{(n)}$ der Congruenz (98), denen

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

nach (101) die aus einem einzigen Gliede bestehende Determinante

$$A = B_\sigma C^\sigma$$

entspricht, wo

$$B_\sigma = b_1' b_2'' \dots b_n^{(n)}, \quad C_\sigma = \sum \pm c_{1,1} c_{2,2} \dots c_{n,n}.$$

Nun kann man aber (nach § 2. I) jede Zahl $b_\nu^{(\nu)}$ aus dem entsprechenden einfachen Modul oder Idealbruch y_ν so auswählen, daß das Ideal $b_\nu^{(\nu)} y_\nu^{-1}$ und folglich auch das Product $B_\sigma Y_\sigma^{-1}$ dieser n Ideale nicht durch p theilbar wird; bezeichnet man dasselbe mit q, so wird $B_\sigma = q Y_\sigma$, also

$$A e^{-1} = B_\sigma C_\sigma e^{-1} = q \cdot Y_\sigma C_\sigma e^{-1},$$

und folglich ist auch das Ideal Ae^{-1} nicht theilbar durch das Primideal p. Hiermit ist offenbar bewiesen, daß $\varepsilon = \sum Ae^{-1}$ der größte gemeinsame Theiler aller Ideale Ae^{-1}, also auch

$$\sum \varepsilon A = e$$

ist, und dies ist zufolge (62) und (104) nur eine andere Form für unseren Satz (95), w. z. b. w.

In dem Falle $m = n$, welcher in den Anwendungen am häufigsten auftritt, nimmt unser Satz (95) offenbar die Form

$$(105) \qquad (\mathfrak{a}; \mathfrak{b})\ X = YC$$

an, wo

$$(106) \qquad Y = y_1 y_2 \dots y_n$$

und

$$(107) \qquad C = \sum \pm c_{1,1} c_{2,2} \dots c_{n,n}$$

ist (vergl. D. S. 523). —

Nachdem hiermit die wichtigsten der auf das neue Symbol (a; b) bezüglichen Sätze bewiesen sind, bemerken wir endlich noch Folgendes. Es ist schon oben (am Schlusse von § 2) erwähnt, daß in dieses Symbol eigentlich die Beziehung der Moduln a, b auf den Körper Z oder auf das System ε aller in Z enthaltenen ganzen Zahlen aufgenommen werden müßte; am einfachsten würde man zu diesem Zweck das Zeichen (a; b) etwa durch (a, b, ε) ersetzen, wo a, b immer solche Moduln bedeuten, welche die Eigenschaft (2) besitzen. In der gegenwärtigen Abhandlung konnte dies der Kürze halber unterbleiben, weil alle Moduln a, b ausschließlich auf diesen einzigen Körper Z bezogen wurden. Die

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

genauere Bezeichnung $(\mathfrak{a}, \mathfrak{b}, \mathfrak{z})$ wird aber nothwendig, wenn mehrere solche Körper betrachtet werden. Nehmen wir z. B. an, es sei Z Divisor eines endlichen Körpers Ω, und $\mathfrak{o}$ das System aller in Ω enthaltenen ganzen Zahlen, so wird jeder Modul $\mathfrak{a}$, welcher der Bedingung $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ genügt, auch die Eigenschaft (2) besitzen, weil $\mathfrak{z} > \mathfrak{o}$ ist. Zwei solche Moduln $\mathfrak{a}$, $\mathfrak{b}$ erzeugen also ein Ideal $(\mathfrak{a}, \mathfrak{b}, \mathfrak{o})$ des Körpers Ω und zugleich ein Ideal $(\mathfrak{a}, \mathfrak{b}, \mathfrak{z})$ des Körpers Z, und unser Satz (31) ist nur ein specieller Fall des allgemeinen Satzes

$$(108) \qquad (\mathfrak{a}, \mathfrak{b}, \mathfrak{z}) = \mathfrak{N}\,(\mathfrak{a}, \mathfrak{b}, \mathfrak{o}),$$

wo $\mathfrak{N}$ das Zeichen für die in Bezug auf Z genommene Partialnorm von Zahlen oder Idealen des Körpers Ω bedeutet. Die ausführliche Darstellung dieser, ebenfalls in der Einleitung erwähnten Untersuchungen muß aber einer besonderen Abhandlung vorbehalten bleiben.

Braunschweig, 4. Februar 1895.

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

http://www.digibib.tu-bs.de/?docid=00053222

Digitale Bibliothek Braunschweig

http://www.digibib.tu-bs.de/?docid=00053222